

## The Identity Theft Cat-and-Mouse Game: An Examination of the State and Federal Governments' Latest Maneuvers

NICKI K. ELGIE\*

**Abstract:** As the sophistication of identity thieves continues to increase, the federal and state governments are faced with the ever-escalating challenge of protecting their citizenry from identity theft. In 2008, several states attempted to meet that challenge by enacting credit freeze laws, joining thirty-seven other states and the District of Columbia that already had such measures in place. Credit freeze laws allow a consumer to freeze his or her credit, thereby preventing a credit reporting agency from releasing the consumer's credit report. Such action is expected to deter new account fraud. The Federal Trade Commission and the federal banking agencies also took a significant step in 2008 to provide protection to American consumers with their adoption of the so-called "Red Flags Rule." This rule should aid in lessening the incidence of both existing and new account fraud by ensuring that financial institutions and creditors keep a watchful eye on the accounts they maintain. While these initiatives are a step in the right direction, the government, at all levels, must continue to develop means of protecting consumers from the risk of identity theft. This will be an ongoing challenge.

---

\* Nicki K. Elgie is a Juris Doctor candidate at The Ohio State University Moritz College of Law, Class of 2009. She earned a Bachelor of Arts degree, *magna cum laude*, in Political Science, with a minor in Sociology, from St. Mary's University. The author has also earned designation as a Certified Information Privacy Professional by the International Association of Privacy Professionals.

## I. INTRODUCTION

Identity theft, fraud committed using the identifying information of another person,<sup>1</sup> has plagued consumers in this country for many years— it is a crisis on the rise.<sup>2</sup> Indeed, it is the fastest growing white collar crime in the country.<sup>3</sup> It exacts a heavy financial burden both on its victims and on our economy in the aggregate.<sup>4</sup> Perhaps the most devastating harm caused by identity theft is suffered by the individual victims, who are faced with considerable difficulties in getting their lives back in order.<sup>5</sup> Also of concern, identity theft results in billions of dollars in losses each year to American businesses.<sup>6</sup>

---

<sup>1</sup> Fair Credit Reporting Act of 1970, 15 U.S.C. §1681a(q)(3) (West 2000 & Supp. 2007).

<sup>2</sup> Between January and December 2007, the complaint database developed and maintained by the Federal Trade Commission (“FTC”) received over 256,000 identity theft complaints. FED. TRADE COMM’N, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA 3 (2008), <http://www.ftc.gov/opa/2008/02/fraud.pdf>. According to the report, the most common form of identity theft was credit card fraud, which accounted for 23% of all complaints. The aggregate consumer loss from all identity theft fraud was over \$1.2 billion. These numbers show a 6.1% increase in reported identity thefts from the previous year; in 2007 the database received about 241,200 identity theft complaints. The reported losses attributable to consumer fraud were reported to be about \$1.1 billion in 2007. *Id.*

<sup>3</sup> DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 126 (Harvard Univ. Press 2008).

<sup>4</sup> Howard Beales, the Director of the Bureau of Consumer Protection of the FTC, testified to as much before the Senate Committee on Banking, Housing, and Urban Affairs: “[I]n addition to harming consumers, [identity theft] also threatens the fair and efficient function of consumer credit markets. It undermines the accuracy and the credibility of the information flows that support those markets.” See S. Rep. No. 108-166, at 8 (2003).

<sup>5</sup> According to the FTC’s 2006 Identity Theft Survey Report, victims of all types of identity theft spend hours of their time resolving the various problems that result from identity theft. Victims spent an average of four hours dealing with the problems that arise after one’s identity is stolen. However, 10% of all victims spent at least fifty-five hours resolving their problems. Further, 5% of victims spent at least 130 hours. SYNOVATE, FEDERAL TRADE COMMISSION— 2006 IDENTITY THEFT SURVEY REPORT 6 (2007), <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

Another source estimates the time costs to be significantly higher, estimating that it takes approximately two years for a victim of identity theft to get his or her identity back in order. According to the same estimate, a victim must devote nearly 200 hours during that two year period to fully regain control over his or her identity. JANINE BENNER, BETH GIVENS & ED MIERZWINSKI, PRIVACY RIGHTS CLEARINGHOUSE, NOWHERE TO TURN: VICTIMS SPEAK OUT ON IDENTITY THEFT (2000), <http://www.privacyrights.org/ar/idtheft2000.htm>.

What's more, as a society, we have been unable to effectively protect citizens from the threat of identity theft.

Both the good news and the bad news is that our failure to curb the identity theft crisis is not a result of government apathy. In fact, both the federal and state governments have recognized the need for a comprehensive solution to identity theft. Over the last decade, the government, at all levels, has grappled with ways in which to curb the growing crisis. Despite their best efforts, identity theft continues to be a major threat to U.S. consumers and has become an increasingly complex and challenging problem for regulators to effectively control; as the government finds more effective means of protecting the identities of its citizens, identity thieves respond by becoming even more clever and sophisticated. Congress and the state legislatures, as well as the regulating authorities, have been playing a cat-and-mouse game with identity thieves. Although federal, state, and local agencies have developed a host of defensive measures over the last decade to counter the ever mounting threats, they seem to have made little progress. Indeed, in 2007, for the seventh consecutive year, identity theft was reported to be the number one consumer complaint in the Federal Trade Commission's ("FTC") list of the top twenty consumer fraud complaints.<sup>7</sup> The difficulty of controlling identity theft has been recognized by Betsy Broder, Assistant Director of the Division of Planning and Information of the Bureau of Consumer Protection, FTC, who lamented that "identity theft often seems unavoidable, undetectable and unstoppable."<sup>8</sup>

In their efforts to keep up with the crisis, state legislative bodies have worked to address ways in which the government can enable individuals to be proactive in protecting their own identities.<sup>9</sup> Most notably in 2008, eight states enacted statutes that allow individuals to

---

<sup>6</sup> THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 11 (2007), <http://www.idtheft.gov/reports/StrategicPlan.pdf> [hereinafter STRATEGIC PLAN]. The Task Force, in its report, explained that businesses suffer most of the direct losses from identity theft because individual victims are not generally held responsible for fraudulent charges. *Id.*

<sup>7</sup> CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, *supra* note 2, at 3.

<sup>8</sup> Betsy Broder, Fed. Trade Comm'n, Prepared Statement on Identity Theft Before the Committee on Banking and Financial Services, United States House of Representatives (2000), [http://www.ftc.gov/os/2000/09/idthefttest.htm#N\\_3](http://www.ftc.gov/os/2000/09/idthefttest.htm#N_3).

<sup>9</sup> The Task Force noted that the first line of defense against identity theft is an aware and motivated consumer that takes reasonable precautions to protect his or her information. STRATEGIC PLAN, *supra* note 6, at 39.

place a freeze on their credit reports, joining thirty-nine other states and the District of Columbia that already had such measures in place.<sup>10</sup> Credit freezes render a consumer's report inaccessible and therefore stop a thief in his or her tracks when the thief attempts to open an account in the victim's name.<sup>11</sup> The 110th Congress also considered several credit freeze bills similar to those enacted in the states. Unfortunately, Congress has yet to enact any measure. A federal credit freeze bill would likely bring much needed uniformity that would increase the utility of credit freezes as a tool for identity theft prevention.

The FTC and the federal financial regulatory agencies ("Agencies")<sup>12</sup> have also been dutifully promulgating rules pursuant to the Fair and Accurate Credit Transaction Act of 2003 ("FACT Act")<sup>13</sup> with the hope of further protecting consumers. In the area of identity theft, the FTC and the Agencies issued final rules entitled *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Transaction Act of 2003* ("Red Flags Rule").<sup>14</sup> The rule,

---

<sup>10</sup> The only states that have not passed a security freeze law are Alabama, Michigan, and Missouri. See FinancialPrivacyNow.org, Consumer Union's Guide to Security Freeze Protection, [http://www.consumersunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html) (last visited Jan. 30, 2009) [hereinafter Consumer Union's Guide].

<sup>11</sup> A security freeze is different from fraud alerts under federal law. As set forth in the Fair Credit Reporting Act, fraud alerts require Credit Reporting Agencies ("CRAs") to scrutinize and monitor alerted accounts for ninety days and to verify the account holder's identity for all credit sought to be extended for that period. 15 U.S.C. § 1681c-1(a)(1). The CRA must also notify all other CRAs of the fraud alert. 15 U.S.C. § 1681c-1(a)(1)(B). A fraud alert attached to a report does not prevent the CRA from issuing a credit report or a credit score. Nor does a fraud alert prevent a CRA from selling or sharing the report with potential creditors. See 15 U.S.C. § 1681c-1(a)(1).

<sup>12</sup> The federal financial regulatory agencies include the banking and securities regulators which are: the Federal Deposit Insurance Corporation, the Federal Reserve Board, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Commodity Futures Trading Commission, and the Securities and Exchange Commission.

<sup>13</sup> Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

<sup>14</sup> Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,717 (Nov. 9, 2007) (to be codified at 12 C.F.R. pt. 41, 12 C.F.R. pt. 222, 12 C.F.R. pts. 334 & 364, 12 C.F.R. pt. 571, 12 C.F.R. pt. 717 and 16 C.F.R. pt. 681), available at <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

which is similar to the Safeguards Rule<sup>15</sup> promulgated under the Gramm-Leach-Bliley Act,<sup>16</sup> requires financial institutions and creditors that hold any consumer account to implement an Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts. The hope is that these programs will ensure that financial institutions and creditors keep a watchful eye on the accounts they maintain; this should provide an added layer of protection to consumers.

In an effort to orient the reader to the ways in which these latest efforts add to the government's attack on identity theft, this note begins by providing a historical overview of identity theft protection in the United States. The note will then devote a section each to the security freeze measures as well as to the Red Flags Rule promulgated under the FACT Act. As with any law or regulation, the final analysis of these initiatives comes down to the extent to which the law or regulation effectively responds to the societal problem that it was designed to correct. Each of the two sections will thus conclude with a discussion of the extent to which the credit freeze measures and the Red Flags Rule are expected to effectively eliminate identity theft: are the cats positioned to finally capture the mice or will the mice once again escape? In response to this question, this note concludes that while these new measures provide some needed protection, the cat-and-mouse game will certainly continue. Defensive measures must continue to evolve in order to keep up with, much less capture, identity thieves.

## II. HISTORICAL OVERVIEW OF IDENTITY THEFT PROTECTION

Congress first began to address issues such as access to information and the unauthorized use of personal data with the Fair Credit Reporting Act ("FCRA") in 1970.<sup>17</sup> The FCRA provided rules regarding permissible purposes for disclosing credit records, procedures for disputing inaccuracies, and basic obligations for credit

---

<sup>15</sup> Safeguards Rule, 16 C.F.R. § 314 (2007). The Safeguards Rule applies to non-bank mortgage lenders, loan brokers, some financial and investment advisers, tax preparers, providers of real estate settlement services, and debt collectors that are "significantly engaged" in financial activities that would trigger the Rule. *Id.*

<sup>16</sup> Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (2006) (codified as amended in 29 U.S.C. § 2903 and scattered sections of 12 U.S.C., 15 U.S.C., 16 U.S.C., and 18 U.S.C.).

<sup>17</sup> 15 U.S.C. § 1681.

users. However, the FCRA did not specifically address identity theft. It was not until the end of the 20th Century that Congress recognized the need for legislation aimed specifically at identity theft.

In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act, which became effective October 30, 1998.<sup>18</sup> The Identity Theft and Assumption Deterrence Act expanded the definition of identity theft to include the misuse of any identifying information, covering misuse of existing accounts as well as the creation of new accounts.<sup>19</sup> Through this law, Congress took two substantial steps toward addressing identity theft. First, the Act made identity theft a federal crime, with penalties of up to fifteen years imprisonment and a maximum fine of \$250,000 for individuals who violate the statute. Secondly, the Act established that individuals whose identities had been stolen were true victims.<sup>20</sup> In order to fulfill the purposes of the Act, the FTC developed a plan to address identity theft, a plan that the Commission has continued to implement. The plan includes a toll-free telephone hotline that consumers can call to report identity theft,<sup>21</sup> as well as the creation of an identity theft complaint database and consumer education programs.

Further protection was provided by the Gramm-Leach-Bliley Act of 1999, a comprehensive piece of legislation affecting financial institutions.<sup>22</sup> Section 521(a) of the Act prohibits obtaining or attempting to obtain customer information of a financial institution relating to another person by fraud or misrepresentation.<sup>23</sup>

Congress's most recent attempt to curtail identity theft was the passage of the FACT Act, which became effective in December 2003.<sup>24</sup> Congress, through the FACT Act, attacked identity theft from several angles, imposing new requirements on entities that maintain

---

<sup>18</sup> Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (2000).

<sup>19</sup> *Id.*

<sup>20</sup> One of the Act's stated goals was to recognize the individual victims of identity theft. See S. Rep. No. 105-274, at 4 (1998). The Act therefore established an assistance process for consumer victims. Prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft.

<sup>21</sup> The identity theft hotline has been in operation since November 1, 1999.

<sup>22</sup> 15 U.S.C. § 6801-6809.

<sup>23</sup> 15 U.S.C. § 6821.

<sup>24</sup> Fair and Accurate Credit Transaction Act of 2003, Pub. L. 108-159, 117 Stat. 1952 (2003).

consumer reporting information and assigning ongoing responsibility for furthering those requirements to the FTC and the federal banking agencies.<sup>25</sup> While the FACT Act and the other federal laws have been helpful in mitigating the harms caused by identity theft, the laws have, for the most part, failed to effectively prevent identity theft.

Recognizing the limits of existing law and initiatives, in 2006, then-President George W. Bush established the Identity Theft Task Force (“Task Force”), which released its Strategic Plan in April 2007.<sup>26</sup> The Task Force included representatives from seventeen federal agencies and departments<sup>27</sup> and was co-chaired by the United States Attorney General and the FTC Chairman. Appropriately, the Task Force recognized that while much had already been accomplished in protecting consumers against identity theft, there remained much room for improvement. Together, the agencies were able to apply a wealth of experience and knowledge to develop a comprehensive plan for combating identity theft. The Task Force, through its Strategic Plan, proceeded to put forth broad recommendations for improvements in four key areas: (1) keeping sensitive consumer data out of the hands of identity thieves through better data security and more accessible education; (2) making it more difficult for identity thieves who obtain consumer data to use it to steal identities; (3) assisting the victims of identity theft in recovering from the crime; and

---

<sup>25</sup> The law imposed requirements on persons who possess or maintain consumer reporting information. 15 U.S.C. §§ 1681b–1681x. It also required the FTC and the federal banking agencies to implement specific rules for the disposal of consumer credit information and records. *Id.* Additionally, the FACT Act required CRAs to maintain reasonable procedures to verify the identity and permissible purposes of those to whom they supply consumer reports. 15 U.S.C. § 1681(e). Consumers were also given the ability to have a fraud alert included in his or her report upon showing of a good faith suspicion of fraud, including identity theft. 15 U.S.C. § 1681c-1(a)(1). Finally, as described more fully in Section V of this note, the FACT Act required the FTC and the federal banking agencies to issue joint rules and guidelines regarding identity theft red flags and address discrepancy. 15 U.S.C. §§ 1681m(e) & 1681c(h)(2)(A).

<sup>26</sup> STRATEGIC PLAN, *supra* note 6. In its introductory material, the Task Force noted that the “problem of identity theft has become more complex and challenging for the general public, the government, and the private sector.” *Id.* at 1.

<sup>27</sup> Those agencies and departments are: Department of Treasury, Department of Commerce, Department of Health and Human Services, Department of Veteran Affairs, Department of Homeland Security, Office of Management and Budget, United States Postal Service, Federal Reserve System, Office of Personnel Management, Federal Deposit Insurance Corporation, Securities and Exchange Commission, National Credit Union Administration, Social Security Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Trade Commission, and the Attorney General.

(4) deterring identity theft with more aggressive prosecution and punishment of those who commit the crime.<sup>28</sup>

In order for our society to have any hope of seeing an end to the crisis, public and private sector action must focus on all four of the key areas identified by the Task Force.<sup>29</sup> Therefore, the continued efforts by the federal and state governments to curtail identity theft can be evaluated in light of the Task Force's comprehensive plan. Those efforts can usually be categorized as focusing on one or more of the four key areas for improvement identified by the Task Force.

Two of those four key areas have been the focus of the state and federal governments' latest maneuvers in the identity theft cat-and-mouse game: making it more difficult for identity thieves to steal identities and assisting victims in their recovery. Over the last year, Congress and the state legislatures have responded to the call of the Task Force, continuing their efforts to keep up with the growing sophistication of identity thieves—both the state credit freeze laws and the Red Flags Rule further the goals identified in the Task Force's Strategic Plan.

### III. CREDIT FREEZES

Much of the identity theft in the United States is a result of “new account” identity theft, through which thieves who have obtained a victim's personally identifiable information, use that information to open a variety of accounts, including credit cards, loans, telephone service, checking accounts and apartment rentals.<sup>30</sup> This sort of identity theft imposes much greater costs on its victims than any other kind.<sup>31</sup> Credit freezes, also referred to as security freezes, have the potential to eliminate, or at least greatly minimize, this form of identity theft. A credit freeze is a consumer protection tool that allows consumers to prevent others from accessing information in their

---

<sup>28</sup> STRATEGIC PLAN, *supra* note 6.

<sup>29</sup> *Id.*

<sup>30</sup> The executive summary of the President's Identity Theft Task Force's Strategic Plan explains that new account fraud occurs when thieves use personal information, such as SSNs, birth dates, and home addresses to open new accounts in the victim's name and proceed to run up charges on those accounts. STRATEGIC PLAN, *supra* note 6, at 3.

<sup>31</sup> *Id.*



credit report, thereby preventing the use of that information to open new accounts.<sup>32</sup>

Credit freeze laws have the ability to address both the second and third of the Task Force's identified goals. Credit freezes make it difficult for identity thieves to use consumer information to open new accounts. As the Task Force recognized, because no security is perfect, and because identity thieves are resourceful, it is essential to reduce opportunities for criminals to misuse data they steal. Credit freezes do just that. If an identity thief is blocked from opening new accounts in a person's name, he or she is likely to be deterred from further attempts at stealing that person's identity. If used only in a reactive capacity, after a consumer's identity has already been stolen, credit freezes help to mitigate any further harm to a consumer's credit. Despite these benefits, credit freezes can be a burdensome tool for protecting consumer identities; their use hinders a consumer's ability to obtain instant credit and requires a fair amount of maintenance.

Over the last five years, state legislatures have jumped on the credit freeze bandwagon, with state after state enacting its own version of the law. The last year has seen a frenzy of such bills before the state legislatures, with eight states enacting credit freeze laws in 2008.<sup>33</sup> Several other states have considered bills that would amend their current credit freeze laws.<sup>34</sup>

This section of the note will first explain the function of security freezes. It will then discuss the state statutes, looking at the procedures involved in placing a freeze, the availability of the measure to consumers, the application of the freeze, and the ancillary protections provided by the state statutes. It will then address the bills before the 110th Congress and the industry-led credit freeze measure. The section will also briefly discuss the current trends in credit freeze laws, as well as examine the future of these measures, both as a creature of state law and as a federal initiative. Finally, the note will turn to the ultimate question: pounce or escape? While

---

<sup>32</sup> A "credit report" is any form of communication of any information by a consumer reporting agency that concerns the consumer's credit worthiness, general reputation, character, manner of living, or personal characteristics with the expectation that the data will be used in order to determine the consumer's eligibility for credit, insurance, employment, or other legitimate business purpose. 15 U.S.C. § 1681a(d).

<sup>33</sup> Those eight states are Alaska, Arizona, Georgia, Idaho, Iowa, Ohio, South Carolina, and Virginia. See Consumer Union's Guide, *supra* note 10.

<sup>34</sup> See, e.g., N.Y. Senate Bill 8376A, 2008 Legis. Sess. (N.Y. 2008) (signed by Governor David Patterson on July 7, 2008).

credit freeze laws have beneficial aspects, it does not appear that the cat will pounce anytime soon.

### A. FUNCTION

Enterprises of all kinds are increasingly requiring access to a consumer's credit report before extending credit, providing services, or even offering a job. As a result, the three major Credit Reporting Agencies ("CRAs")<sup>35</sup> have extensive information about almost every American.<sup>36</sup> Not surprisingly, one of the contributing factors in the identity theft crisis is that the CRAs and the business entities that maintain personal information on consumers often lack the incentives to adequately protect the personally identifiable information they possess.<sup>37</sup> Even given the proper incentives, these entities have few effective means of controlling access to the records and accounts they maintain.<sup>38</sup> Credit freeze laws partially fill that gap.

Credit freeze laws are intended to empower consumers to protect themselves against identity theft.<sup>39</sup> In placing a freeze on his or her

---

<sup>35</sup> CRAs include the three major credit bureaus as well as other specialized agencies that collect and compile information about a consumer's creditworthiness. For an in depth discussion of credit reporting systems, both in the United States and internationally, see NICOLA JENTZSCH, *FINANCIAL PRIVACY: AN INTERNATIONAL COMPARISON OF CREDIT REPORTING SYSTEMS* (2d ed. 2007).

<sup>36</sup> SOLOVE, *supra* note 3, at 5. Experian maintains credit information on approximately 215 million U.S. consumers and more than 15 million U.S. businesses. Experian Corporate Fact Sheet, <http://www.experian.com/corporate/factsheet.html> (last visited Jan. 30, 2009). TransUnion maintains credit histories on an estimated 500 million consumers around the globe. TransUnion, Fast Facts, <http://www.transunion.com/corporate/aboutUs/aboutUs.page> (last visited Jan. 30, 2009).

<sup>37</sup> SOLOVE, *supra* note 3, at 127. U.S. Secret Service Special Agent Timothy Caddigan elaborated on this point to the Senate Committee on Banking, Housing and Urban Affairs: "The burgeoning use of the Internet and advanced technology, coupled with the increased investment and expansion, has intensified competition within the financial sector. Although this provides benefit to the consumer through readily available credit and consumer-oriented financial services, it also creates a target-rich environment for today's sophisticated criminals. . . ." See S. Rep. No. 108-166, at 8 (2003).

<sup>38</sup> Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 90 (2001-2002).

<sup>39</sup> For example, the Rhode Island statute explains that the measure establishes the right of consumers "to protect themselves from identity theft or fraud by conferring upon them the right to voluntarily place a security freeze on their credit report." R.I. GEN. LAWS § 6-48-2 (2001 & Supp. 2007).

credit report, a consumer has the ability to eliminate new account identity theft because businesses typically will not extend new credit or provide other benefits without first viewing an applicant's credit report.<sup>40</sup> A credit freeze prohibits a CRA<sup>41</sup> from releasing the consumer report or credit score of the consumer in response to a request. It thereby blocks any access to the credit report and thus effectively stops any attempt to open a new account. At that point, an identity thief is unlikely to proceed with any efforts to steal the identity of that particular consumer.

## B. STATE STATUTES<sup>42</sup>

California enacted the country's first credit freeze law in 2001, although the law did not become effective until January 1, 2003.<sup>43</sup> Texas, Louisiana, and Vermont quickly followed suit.<sup>44</sup> In 2005, other states began passing similar laws in response to extensive data breaches across the country. In fact, many of the states passed laws which included credit freeze provisions as well as data breach notification provisions in the same piece of legislation. All fifty states

---

<sup>40</sup> Fed. Trade Comm'n, Impact and Effectiveness of Credit Report Freezes: Topics for Comment (Jan. 11, 2008), *available at* <http://www.ftc.gov/opa/2008/01/freeze.pdf> [hereinafter FTC Request for Comment]. The FTC solicited comments in response to the strategic plan issued by the President's Identity Theft Task Force, which recommended that the FTC assess the impact and effectiveness of credit freeze laws. Evidently, the recommendation was made with the hope that the results would assist policymakers in considering the appropriateness of a federal credit freeze law. *See* STRATEGIC PLAN, *supra* note 6, at 52. For one group's responses to the FTC's request for comments, *see* Letter from Cutler Dawson, President and CEO, Navy Federal Credit Union, to FTC (Feb. 25, 2008), *available at* <http://www.ftc.gov/os/comments/creditreportfreezes/534030-00048.pdf>.

<sup>41</sup> Most of the states, in their credit freeze statutes, adopted the FCRA definition of a credit reporting agency: "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

<sup>42</sup> *See* Appendix A for a table outlining the various components of all fifty states' statutes. The Appendix is current as of January 1, 2009.

<sup>43</sup> CAL. CIV. CODE § 1785.11.2 (West 1998 & Supp. 2008).

<sup>44</sup> TEX. BUS. & COM. CODE ANN. § 20.01 (Vernon 2002 & Supp. 2007); LA. CIV. CODE ANN. art. 9 § 3571.1 (2008); VT. STAT. ANN. tit. 9, § 2480h (2006).

and the District of Columbia either have a credit freeze law on the books or have had a measure to create such a law before their respective legislatures.<sup>45</sup>

While the state laws all have the same goal and follow the same basic model, they differ in several respects. Some of these differences include whether all consumers, or only those who are victims of identity theft, can obtain a freeze, the amount credit reporting agencies may charge consumers for freezing, temporarily lifting (sometimes referred to as “thawing”), or removing a freeze on an account, and the length of time allotted CRAs to comply with consumer requests to freeze or thaw their credit reports.

#### 1. AVAILABILITY AND PROCEDURES/COST FOR PLACING, TEMPORARILY LIFTING, AND REMOVING

Generally, the statutes extend the right to place a credit freeze to all of the state’s residents. However, four states currently limit that right to identity theft victims.<sup>46</sup> The state lawmakers have almost uniformly recognized that all consumers should benefit from these laws. In fact, the laws make little sense unless they provide protection to all consumers; otherwise they are relegated to the status of a reactive tool rather than a proactive one.

Pursuant to most of the state statutes, a consumer wishing to place a freeze on his or her credit report must send a written request to each

---

<sup>45</sup> The most up-to-date, interactive list of state credit freeze laws can be found on the Consumer Union’s website at [www.consumerunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumerunion.org/campaigns/learn_more/003484indiv.html) (last visited Jan. 30, 2009). However, given the onslaught of state legislation expected over the next year it may not be 100% accurate. It was last updated on September 30, 2008.

<sup>46</sup> The four states are Arkansas, Kansas, Mississippi, and South Dakota. ARK. CODE ANN. §4-112-101 (2001 & Supp. 2007); KAN. STAT. ANN. § 50-723(a) (2008); MISS. CODE ANN. § 75-24-201(1) (West 1999 & Supp. 2007); S.D. CODIFIED LAWS § 54-15-13 (2004 & Supp. 2008). Washington’s statute limited credit freezes to identity theft victims until September 1, 2008; credit freezes are now available to all consumers. WASH. REV. CODE § 19.182.170 (2007 & Supp. 2008). In 2008, Mississippi and South Dakota both had bills introduced in their respective legislatures that would have allowed all residents the benefit of the statute; unfortunately those bills failed to become law. See H.B. 574, Gen. Assem., Reg. Sess. (Miss. 2008) (declared dead in committee Feb. 19, 2008); H.B. 1036, Gen. Assem., Reg. Sess. (Miss. 2008) (declared dead in committee Feb. 19, 2008); S.B. 81, 2008 Leg., 83d Sess. (S.D. 2008) (gained committee approval but failed to be taken up on the floor when the Legislature adjourned for the year). The Kansas legislature also considered a bill to expand the state’s credit freeze law. H.B. 2880, 2008 Legis. Sess. (Kan. 2008) (referred to Insurance and Financial Institutions Committee).

CRA in order to have a freeze placed on his or her account.<sup>47</sup> Most statutes currently require that the request be sent by certified mail,<sup>48</sup> but state lawmakers are increasingly pushing to have the CRAs develop a means to accept electronic requests<sup>49</sup> or otherwise make it easier for a consumer to request a freeze.<sup>50</sup> At present, consumers must contact each of the CRAs separately to request a freeze.

The great majority of the statutes provide that a freeze will stay in effect until such time as the consumer requests that it be removed.<sup>51</sup> However, four state statutes provide that a credit freeze must be removed seven years after the date on which it was first placed if not already removed by the consumer.<sup>52</sup> Freezes can also be temporarily lifted so that one's credit report can be made available to a specific party or for a specific time period.<sup>53</sup> Many of the states only allow consumers to lift a freeze for a specific amount of time, but a number of states also provide that a consumer can lift a freeze for a specific

---

<sup>47</sup> The CRAs typically require consumers requesting a security freeze to provide a combination of personal identification sources in addition to their full name and address (i.e., SSN, date of birth, copy of driver's license, and/or a copy of a bill or secondary proof of address). In addition, identity theft victims must include a copy of the police report or other verification of their claim.

<sup>48</sup> See, e.g., ARK. CODE ANN. §4-112-103(a)(1) (2001 & Supp. 2007).

<sup>49</sup> For example, the Delaware statute requires the consumer reporting agencies to have made an electronic mail method available by January 31, 2009. DEL. CODE ANN. tit. 6 § 2203(b)(1) (2005 & Supp. 2006); see also IND. CODE § 24-5-24-5(d) (West 2006 & Supp. 2008) (electronic method required by January 1, 2009).

<sup>50</sup> Minnesota allows a consumer to place a freeze using a toll-free number. MINN. STAT. § 13C.016(c)(2) (2005 & Supp. 2008). The recently amended California statute allows consumers to send a request via regular mail rather than certified. CAL. CIV. CODE § 1785.11.2(a) (West 1998 & Supp. 2008).

<sup>51</sup> See, e.g., Sub. H.B. 46, 127th Gen. Ass. (Ohio 2008) (enacted) (codified OHIO REV. CODE ANN. § 1349.52(G)).

<sup>52</sup> The four states are Kentucky, Nebraska, Pennsylvania, and South Dakota. KY. REV. STAT. ANN. § 367.365(8) (West 2008); NEB. REV. STAT. § 8-2607(1) (2003 & Supp. 2008); 73 PA. CONS. STAT. § 2503(d) (2008); S.D. CODIFIED LAWS § 54-15-11 (2004 & Supp. 2008).

<sup>53</sup> In order to have a CRA temporarily lift a freeze, the consumer must usually provide each CRA with proper identification, the unique personal identification number given to the consumer when the freeze was first placed, proper information regarding the third party who is to receive the credit report or the time period for which the report is to be made available, and a fee, if applicable. See, e.g., N.Y. GEN. BUS. LAW § 380-t(c) (McKinney 1996 & Supp. 2008).

party.<sup>54</sup> The statutes provide that the CRAs are free to develop their own procedures for receiving and processing requests from consumers to lift a freeze from their account. Many provide, however, that these procedures must at least include the ability of a consumer to send requests by electronic mail, letter, or facsimile.<sup>55</sup>

Every statute also mandates a time period within which a CRA must process and implement a consumer's request, whether that be to place, temporarily lift, or remove a freeze. These time periods range from fifteen minutes to several days and differ depending on the action the consumer requests; CRAs are usually given longer to implement the initial freeze and less time to temporarily lift a freeze.<sup>56</sup> The trend is to shorten the deadline over time. Some state statutes provide that after a certain future date, the time limit will be lessened. Similarly, other states are considering amending their statutes to reduce the amount of time a CRA has to implement requests.<sup>57</sup> Presumably, these time periods are lessened as the CRAs are able to develop procedures and mechanisms to effectively implement freezes and later remove those freezes.

An important aspect of the state laws, especially in the minds of most consumers, is the cost of placing a freeze and thereafter managing one's credit report. Most state statutes allow the CRAs to

---

<sup>54</sup> Montana is one of the several states that allow a consumer to allow access to the consumer's report to a specific party or for a specific period of time while the security freeze is in place. MONT. CODE ANN. § 30-14-1729 (2007).

<sup>55</sup> See, e.g., CONN. GEN. STAT. § 36a-701a(d) (2004 & Supp. 2008).

<sup>56</sup> Kentucky, Louisiana and Arizona currently allow CRAs the longest period of time to comply with a consumer's request to place a freeze—10 days. KY. REV. STAT. ANN. § 367.365(1)(a) (LexisNexis 2002 & Supp. 2007); LA. CIV. CODE ANN. art. 9§ 3571.1 M(1) (1997 & Supp. 2008); ARIZ. REV. STAT. ANN. § 44-1698(B) (2003 & Supp. 2008). Montana's statute provides the least amount of time for a CRA to respond to an initial freeze request—twenty-four hours—but that only applies to requests from victims of identity theft. Otherwise the CRAs have five business days to respond. MONT. CODE ANN. § 30-14-1728 (2008). The remaining states allow the CRAs either three or five business days to comply with an initial request. Utah is one of the many states that allow a CRA only fifteen minutes to respond to a consumer's electronic request to temporarily lift a freeze. UTAH CODE ANN. § 13-45-202 (2008).

<sup>57</sup> For instance, New York's recently amended statute provides that beginning January 1, 2010, a CRA will be required to place a freeze on a consumer report within twenty-four hours of receiving the request. N.Y. GEN. BUS. LAW § 380-t(b) (McKinney 1996 & Supp. 2008). The original law, which became effective in 2006, gave CRAs four business days to place a freeze through the end of 2008, and, beginning January 1, 2009, gave three business days.

charge a fee to place, temporarily lift, or remove a freeze, usually around ten dollars for each of these transactions, although the permitted fees vary from state to state. Many of the statutes also provide that the maximum fee amount shall be increased at the end of each year based on the Consumer Price Index.<sup>58</sup> Indiana, Kansas, South Carolina, and South Dakota are the only states that do not permit, or at least do not specifically allow, the CRAs to charge consumers a fee.<sup>59</sup> The trend has been to decrease the fees that CRAs are allowed to charge. Despite the general allowance for reasonable fees, most states do not allow CRAs to charge fees to identity theft victims.<sup>60</sup> Several states also do not allow fees to be charged to individuals over the age of sixty-five or to active military personnel.<sup>61</sup>

## 2. EXTENT OF APPLICATION AND EXCEPTIONS

Credit freezes do not limit all access to a consumer's credit report. For instance, credit freezes do not apply to the use of a consumer credit report by a person or entity with which a consumer has an existing account that requests information in the consumer's credit report for purposes of reviewing or collecting the account; a person acting pursuant to a court order, warrant, or subpoena; a state or local agency that administers child support obligations; or the Department of Justice, law enforcement agencies, and the Department of Health and Social Services.<sup>62</sup> Further, credit freezes do not prevent a CRA from advising a third party that a credit freeze is in effect with respect to the consumer report.<sup>63</sup> Importantly, the consumer is still able to access his or her credit and remains able to access a free annual credit

---

<sup>58</sup> See, e.g., TEX. BUS. & COM. CODE ANN. § 20.04(a) (Vernon 2002 & Supp. 2008).

<sup>59</sup> IND CODE § 24-5-24-1 (West 2006 & Supp. 2008); KAN. STAT. ANN. § 50-723, et seq. (2008); S.C. CODE ANN. §37-20-160 (2008); S.D. CODIFIED LAWS § 54-15-1 (2004 & Supp. 2008).

<sup>60</sup> See, e.g., GA. CODE ANN. § 10-1-914(p) (2008).

<sup>61</sup> See, e.g., *id.*

<sup>62</sup> See, e.g., DEL. CODE ANN. tit. 6, § 2203(b)(12) (2005 & Supp. 2006).

<sup>63</sup> See, e.g., COLO. REV. STAT. § 12-14.3-106.6(c) (2007). Nor do they prevent a third party that requests a report which is frozen from treating the application as incomplete. *Id.*

report. Finally, not all entities are required to place a credit freeze requested by a consumer.<sup>64</sup>

### 3. DUTIES OF CREDIT REPORTING AGENCIES/ANCILLARY PROTECTIONS PROVIDED UNDER THE STATUTES

Aside from responding to consumer requests within a specified period of time, CRAs have several other duties pursuant to the state laws that provide ancillary protections to consumers. First, most of the statutes provide for the issuance of a notice outlining a consumer's right to obtain a credit freeze, a notice that must be included whenever a consumer is required to receive a summary of rights under the Fair Credit Reporting Act.<sup>65</sup> These notices provide consumers with a summary of their rights as well as the procedures for placing a freeze and managing their credit reports thereafter.

Further, every state statute provides that when a credit report is subject to a credit freeze, the CRA must, within thirty days, notify the consumer whose report is frozen if the CRA substantially changes the consumer's information.<sup>66</sup> Thus, the CRA must notify the consumer if the consumer's name, date of birth, social security number, and/or address is changed. This requirement will ensure that the consumer is made aware of unauthorized changes to his or her personal information.

### 4. PENALTIES FOR VIOLATIONS

Most states provide a private cause of action for damages caused by a CRA's failure to adhere to the credit freeze laws.<sup>67</sup> Other states,

---

<sup>64</sup> The following entities are not required to place a freeze on a consumer report: (1) consumer reporting agencies that act only as resellers of credit information by assembling and merging information contained in the database of another consumer reporting agency; (2) check services or fraud prevention services companies; and (3) deposit account information service companies. *See, e.g., id.*

<sup>65</sup> *See, e.g.,* OKLA. STAT. tit. 24 § 158 (2008).

<sup>66</sup> A consumer's information may be changed, despite a credit freeze being in place, in such instances as when the consumer changes that information or when an identity thief attempts to do so; a credit freeze only blocks information being released by a CRA, not any information provided to the CRA.

<sup>67</sup> A partial list of states that provide an individual right of action include: Colorado, Delaware, Florida, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maryland, Ohio, Virginia, West Virginia, Wisconsin, and Wyoming. Wyoming provides a right to a civil action only if the CRA violates the statute, then fails to take steps to correct the release of the credit



however, give the state Attorney General exclusive authority to enforce the provisions of the statute.<sup>68</sup> The scheme for punishing violators is relatively similar in every state that provides for an individual cause of action. Most states distinguish between willful and negligent violations. The majority of those states provide that willful violators will be liable for actual damages, with some limits,<sup>69</sup> as well as punitive damages,<sup>70</sup> costs, and reasonable attorneys' fees. An entity that is merely negligent in failing to comply with a credit freeze law is liable to the injured party for only actual damages along with the costs of the action and reasonable attorneys' fees. South Carolina's statute is an example of a provision providing unusually high statutory damages, allowing up to \$3000 for each negligent violation and the greater of three times actual damages or \$5000 per willful violation.<sup>71</sup>

In addition, the statutes also provide monetary penalties for individuals who, under false pretenses, obtain a consumer report, request a security freeze, request a temporary lift of a freeze, or request the removal of a security freeze. Pursuant to most state laws, such an individual is liable to the CRA for actual damages.

## 5. TRENDS

As alluded to throughout the discussion of the credit freeze laws, there are six major trends in the credit freeze laws: (1) lowering or prohibiting fees charged to consumers for placing, temporarily lifting, or removing a freeze; (2) expanding freeze laws to make freezes available to all consumers; (3) allowing consumers to temporarily lift a freeze for specific individuals or entities requesting their credit

---

report and further fails to give notification to the consumer. WYO. STAT. ANN. § 40-12-508 (2007).

<sup>68</sup> See, e.g., 73 PA. CONS. STAT. § 2510 (1993 & Supp. 2007) (providing that a violation of the security freeze statutes shall be deemed to be an unfair or deceptive act or practice in violation of the Unfair Trade Practices and Consumer Protection Law, giving the Attorney General exclusive authority to bring such an action).

<sup>69</sup> Usually, individuals are entitled to actual damages of not less than \$100 and not more than \$1000. See, e.g., VA. CODE ANN. § 59.1-444.2(Q) (2006 & Supp. 2008).

<sup>70</sup> A partial list of states that have statutes specifically allowing courts to grant punitive damages to individuals for a CRA's willful violation of the law include Alaska, Virginia, Idaho, Indiana, Kansas, Kentucky, Montana, New Mexico, Tennessee, and the District of Columbia. Georgia and Arizona specifically do not allow for punitive damages.

<sup>71</sup> S.C. CODE ANN. § 37-20-110, et. seq. (2008).

reports, rather than for a specified length of time only; (4) increasingly requiring CRAs to make available an electronic means of requesting the placement, lift, or removal of a freeze or otherwise making it easier for consumers to make freeze-related requests; (5) decreasing the amount of time a CRA has to respond to a consumer request; and (6) increasing penalties for violation of the applicable statute.<sup>72</sup>

### C. INDUSTRY-INITIATED CREDIT FREEZES

The three major CRAs, Equifax, Experian, and TransUnion, offer credit security freezes as a service to consumers who are residents of the states that have no credit freeze laws and to all residents in the four states where the right to freeze under state law only applies to identity theft victims.<sup>73</sup> The population that will take advantage of the industry-initiated freezes is rapidly dwindling as more states are

---

<sup>72</sup> Two cases in point are the recently enacted Virginia statute and the recently amended California law. The Virginia statute, which became effective on July 1, 2008, allows CRAs three business days to respond to a consumer's initial request to place a freeze; however, beginning July 1, 2009, a CRA will only have twenty-four hours to respond. VA. CODE ANN. § 59.1-444.2(B) (2006 & Supp. 2008). Further, pursuant to the new Virginia law, a CRA can charge ten dollars for placing a security freeze on a consumer's report, but cannot charge any other fees to later temporarily lift or remove the freeze. *Id.* The Virginia law allows CRAs only fifteen minutes to respond to a consumer's request to temporarily lift a freeze if that request was received electronically. VA. CODE ANN. § 59.1-444.2(E)(1)(b). Finally, the law allows the consumer to request that the CRA temporarily lift a freeze for either a period of time or for a specific party. VA. CODE ANN. § 59.1-444.2(D)(3). The California amendment, which became effective January 1, 2009, also showcases several of the trends. It requires that CRAs accept freeze requests by regular mail rather than by certified mail only. It also shortens the time a CRA has to place a freeze from five to three days. Allowable fees are also decreased. Specifically, the fee to temporarily lift the freeze for a specific party is decreased by two dollars. Also, the amendment requires that consumers sixty-five years or older be charged no more than five dollars per request. The amendment also made changes to the written summary of rights that a CRA is required to provide to a consumer. See A.B. 372, 2007-08 Reg. Sess. (Cal. 2008) (amending CAL. CIV. CODE §§ 1785.11.2 & 1785.15).

<sup>73</sup> See PRNewswire, *TransUnion First to Announce File Freeze Option in all 50 States*, D.C., Sept. 18, 2007, <http://newsroom.transunion.com/index.php?s=43&item=432>. Since the initial announcement, the three main CRAs have developed more extensive services for individuals to freeze and otherwise manage their credit reports. For example, Equifax offers its Credit Report Control to consumers for \$14.95 per month; this service allows a consumer to manage the freeze status of his or her report online, enabling the consumer to lock or unlock a report with the click of a mouse. The consumer is able to unlock a credit freeze for a period of time or for specific businesses. Equifax Credit Report Control, <http://www.equifax.com/credit-report-lock> (last visited Feb. 8, 2009).

enacting credit freeze bills or amending their prior statutes to give all consumers the ability to place a freeze on their accounts. The fees under the initial industry-initiative are ten dollars for each request to place a freeze, temporarily lift a freeze, or permanently remove the freeze, although the CRAs have individually developed more complex services that vary in cost.<sup>74</sup> The CRA-developed freeze options are not well advertised and there is no data evidencing their utilization. However, services like Equifax's Credit Report Control offer a consumer the benefit of monitoring his or her credit freeze for a flat fee. These services may also prove to be more conducive to the realities of the credit reporting industry as they are created by the CRAs themselves.

#### D. POSSIBLE FEDERAL CREDIT FREEZE LAW

Congress has considered several bills that would create a federal credit freeze law. Unfortunately, none of the federal measures would preempt the state freeze laws. These bills would, nonetheless, have the benefit of providing a comprehensive approach to credit freezes for consumers all across the country.

The federal bills are substantially similar to those of the states, but do provide certain benefits above those provided for in the state statutes. Indeed, the federal bills have the benefit of experience, and largely reflect what has been learned from the response to the state laws. Notably before the 110th Congress were the Identity Theft Prevention Act of 2007, H.R. 3316,<sup>75</sup> the Identity Theft Prevention Act, S. 1178,<sup>76</sup> and the Consumer Identity Theft Protection and Security Act, S. 806.<sup>77</sup>

These bills are quite similar, but each provides certain advantages over the others. H.R. 3316, which proposes to amend the FCRA, would make placing a security freeze more convenient by providing that a method be established through which an individual could make a single request to place a freeze on his or her credit rather than

---

<sup>74</sup> See e.g., *TransUnion First to Announce File Freeze Option in all 50 States, D.C.*, *supra* note 73; Consumer Union's Guide, *supra* note 10.

<sup>75</sup> H.R. 3316, 110th Cong. § 2 (2007) (stalled in the Subcommittee on Financial Institutions and Consumer Credit).

<sup>76</sup> S. 1178, 110th Cong. § 4 (2007) (placed on the Senate Legislative Calendar, but has not been subject to a vote).

<sup>77</sup> S. 806, 110th Cong. § 2 (2007) (remains in committee).

contacting each of the CRAs individually. S. 1178 would make credit freezes more manageable by allowing a consumer who has requested a credit freeze to temporarily lift it at no cost up to two times every year.<sup>78</sup> S. 1178 and S. 806 would also exempt identity theft victims, all individuals over the age of 65, those in active military duty, and the spouses of those in active duty from paying a fee to freeze their credit reports. S. 806 would allow the highest fees: fifteen dollars to place, remove, or temporarily lift. Otherwise, the federal bills look very much like the state laws. Still, despite having only subtle differences, a national credit freeze law would be beneficial to the extent that it provides uniformity.

#### E. POUNCE OR ESCAPE?

The Task Force identified credit freezes as victim recovery measures—essentially a means by which victims of identity theft can mitigate harm after their identities have been stolen. This is certainly one aspect of the freeze laws. However, the success of these initiatives would likely be increased if they were promoted in a way that would encompass the second of the Task Force's goals—which is a more proactive approach to curbing identity theft—to make it more difficult for identity thieves who obtain consumer data to ultimately use it to steal identities. Thus, credit freezes need to also be viewed as a preventative measure. Most states recognize this aspect of the freezes by allowing all consumers to request a freeze rather than limiting the right to identity theft victims only. Yet, the freeze laws are largely promoted as a response to identity theft, not a way of preventing it in the first place. Whether viewed as a purely reactive measure, or as a preventative measure, the prognosis for these laws is the same: while a useful tool, the credit freeze laws are only a small piece of the puzzle in this cat-and-mouse game.

As noted in the Task Force's strategic plan, because the state freeze laws are relatively new, there is little data with which to measure their effectiveness.<sup>79</sup> There has not been any targeted research aimed at measuring the extent to which security freeze laws can be credited with preventing identity theft. However, the FTC solicited comments on the impact and effectiveness of credit freezes in early January 2008.<sup>80</sup> The FTC sought public comment on the extent

---

<sup>78</sup> S. 1178, 110th Cong. § 4(h)(1).

<sup>79</sup> STRATEGIC PLAN, *supra* note 6, at 52.

<sup>80</sup> FTC Request for Comment, *supra* note 40.

to which credit freezes were effective in preventing identity theft, the types of identity theft credit freezes prevented, whether there are aspects of the credit freeze laws that encourage or hinder their use, how the CRA-developed freeze options compare in practice to the state laws, and the beneficial and burdensome effects of credit freezes on consumers, businesses, and the economy. The Commission should issue a report in the coming months, and the responses the Commission receives should provide valuable insight into the effectiveness of the credit freezes providing instruction for future developments.

Even without the FTC's report, it is possible to draw some conclusions about the effectiveness of these laws, based on preliminary research regarding consumer awareness about credit freezes and based on normal human behavior. An obvious downside to the credit freezes is the hassle that attaches to their application.<sup>81</sup> As recognized by the California lawmakers, "[t]he cost and complexity of placing and lifting security freezes are . . . significant barriers to the use of this protection against identity theft."<sup>82</sup> For instance, it is impossible for a consumer to obtain so-called "instant credit" if a credit freeze is in effect. As discussed above, the consumer must contact each of the CRAs individually and pay the applicable fees before the freeze is temporarily lifted or removed. At that point, under most current state laws, the CRA has three business days to remove the credit freeze. This limitation may cause many consumers to forego placing a freeze. Additionally, the fees, while moderate, add up quickly. In most states there is a fee for placement of a freeze and for every subsequent lifting of the freeze. Moreover, the applicable fees must be paid to each CRA separately. A study conducted by AARP in mid-2007, which explored consumer use of credit freezes, identified fees as a major barrier to the success of credit freeze laws.<sup>83</sup>

---

<sup>81</sup> The Massachusetts consumer notice of rights under the state's security freeze law lists several of the possible inconveniences: "[u]sing a security freeze may delay, interfere with, or prevent the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions, or other services, including an extension of credit at point of sale." MASS. GEN. LAWS ch. 93 § 52 (2005 & Supp. 2008).

<sup>82</sup> MARK FAROUK, BILL ANALYSIS OF A.B. 372, 2007–08 Reg. Sess. (Cal. 2008).

<sup>83</sup> JENNIFER H. SAUER & NEAL WALTERS, AARP, SECURITY FREEZE LEGISLATION: AWARENESS AND INCIDENCE OF PLACEMENT AMONG CONSUMERS 18+ IN SEVEN STATES (2007), [http://assets.aarp.org/rgcenter/consume/freeze\\_leg.pdf](http://assets.aarp.org/rgcenter/consume/freeze_leg.pdf). Of 6534 consumers questioned, only fourteen percent said they would be extremely or very likely to place a freeze on their report if they had to pay ten dollars to each CRA. Nearly 60% said that they would unlikely

Finally, continuously keeping up with the status of one's credit reports can be an arduous task for the modern consumer.

As a result of these limitations, the security freezes may not be taken advantage of by the average consumer. In adopting credit freeze provisions, the states followed the FACT Act by placing the burden of protecting one's identity on the consumer, a trend that probably gives identity thieves an advantage in the cat-and-mouse game. While the American public has become increasingly concerned about privacy, studies show that there is a dichotomy between privacy attitudes and actual behavior.<sup>84</sup> The state security freeze laws may not adequately consider the decision-making behavior and biases of the average American.

For example, a person's credit history is becoming increasingly critical to that person's ability to function in everyday life. Placing, lifting, and replacing security freezes each time an individual needs to provide access to his or her credit report imposes a significant burden on consumers. Again, the newness of the state credit freeze laws forecloses the existence of any comprehensive studies analyzing their utilization. However, much can be learned from studies analyzing the instances in which individuals take advantage of the ability to place a fraud alert on their credit report after receiving notice of a data breach. Only a minority of individuals that are notified of a data breach ever break ties with the business that was to blame for the breach—far fewer take the extra step to place fraud alerts on their credit reports.<sup>85</sup> There are probably three main reasons for this phenomenon, all of which apply with equal force to the credit freeze laws. First, individuals have busy lives and just cannot be bothered with the inconvenience. Second, individuals likely do not view the risk of identity theft as serious enough to warrant the extra effort; as the immediacy of the threat declines, consumer vigilance tends to

---

take advantage of the freeze laws if they had to pay a ten dollar fee. Those numbers became even more dire when respondents were asked to consider the fees associated with temporarily lifting a freeze. *Id.* at 9.

<sup>84</sup> Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY* 15, 16 (Katherine Strandburg & Daniela Stan Raicu eds., 2006). Acquisti and Grossklags postulate that individuals are willing to trade privacy for convenience. *See also* SAUER & WALTERS, *supra* note 83.

<sup>85</sup> In their survey, Acquisti and Grossklags found that among individuals who reported being particularly concerned about credit card fraud and identity theft, only 25.9% used credit alert features. Acquisti & Grossklags, *supra* note 84, at 23.

atrophy.<sup>86</sup> Finally, despite the governments' best efforts, individuals may not even know about their options with regard to protecting their identities.<sup>87</sup> The AARP study, for instance, concluded that while there is high concern about identity theft, both awareness of the credit freeze laws and their utilization is extremely low.<sup>88</sup>

Also, while credit freezes are helpful in keeping identity thieves from opening most new accounts in another's name, they are certainly less useful, if at all, in preventing other types of identity theft such as existing account fraud. Given the lack of familiarity with the freeze laws, the expense and inconvenience associated with managing the status of one's credit report, and the tendency of consumers to be apathetic in proactively protecting their identities, it is not surprising that the AARP study found that less than 1% of all respondents across the seven states surveyed indicated that they were currently utilizing the credit freeze laws.<sup>89</sup>

A final shortcoming to the state statutes is that, although the laws are similar in many regards, the variations can make CRA compliance excessively complicated. The CRAs must spend an enormous amount of time and resources ensuring compliance with each of the statutes. Again, a federal law would likely simplify the process. Unfortunately, progress at the federal level has been slow and even if a federal law is enacted, it is unlikely to preempt state laws.

---

<sup>86</sup> The Acquisti and Grossklags study suggests that the instances in which individuals will take protective measures against identity theft will decrease with the length of time before one would expect to incur the damages from privacy intrusions. *Id.* at 28. This lack of response is similar to that seen when severe weather alerts are issued. Alarms go off, but many people ignore them. Either they have heard too many warnings without corresponding harm to actually heed those warnings, or, after weighing the risk of severe weather actually occurring against the inconvenience of stopping what they are doing and seeking shelter, they decide that the risk is not great enough to go through the inconvenience. Either way, the warning is disregarded. Ninety-nine times out of a hundred those individuals will probably be fine, but the consequences of not heeding a warning are readily apparent. Individuals take a similar approach with protecting their identities and often face the consequence of identity theft.

<sup>87</sup> Fifty-four percent of the respondents in the Acquisti and Grossklags study could not cite any law that influenced or impacted privacy. Acquisti & Grossklags, *supra* note 84, at 25.

<sup>88</sup> SAUER & WALTERS, *supra* note 83, at 7. The majority of the 8412 respondents (62%) in the AARP study either did not know of or were not sure if they had heard of the right to place a security freeze on a consumer report. Among those respondents who had not heard of security freeze laws, only 2% were able to identify the name of the service. *Id.*

<sup>89</sup> *Id.* at 8.

It is apparent that, while great in theory, the credit freeze laws are under-utilized. This may be due in part to the fact that the freezes have not been marketed appropriately; they are promoted as a means of mitigating damages once a person has become a victim of identity theft. Consumer groups, as well as the Task Force, have failed to recognize the utility of a credit freeze to prevent identity theft in the first place. The proper and more efficient role of a credit freeze would be as a proactive means for all consumers to protect their identities in case their personally identifiable information is stolen at some point in the future. Unfortunately, given the burden of managing one's credit report, the proactive aspect of credit freezes may never be fully utilized.

In order to be more effective, the credit freeze laws must continue to evolve, following the six trends identified above. Ideally, this evolution will lessen the consumer burden of managing the placement of a freeze on one's credit report and thereby encourage consumers to fully utilize credit freezes as a protective measure. Further, Congress should consider enacting a federal law that would preempt state laws. The provisions of the federal initiatives, taken together, would eliminate much of the financial and time burdens thought to decrease the utilization of the credit freezes. A federal law that preempts state law would ensure a comprehensive national standard, providing much needed clarity and predictability to consumers and CRAs alike.<sup>90</sup>

#### IV. FACT ACT REGULATION: THE RED FLAGS RULE

The FACT Act<sup>91</sup> added several new provisions to the Fair Credit Reporting Act of 1970 ("FCRA")<sup>92</sup> in an effort to enhance the ability of consumers to combat identity theft and enhance the accuracy of consumer report information. As discussed above, although the FCRA targeted the information industry, it did not provide the necessary tools to protect consumers from identity theft; the FACT Act was a response to this void in the law. Most important for the purposes of this note, the FACT Act required the FTC and the federal banking

---

<sup>90</sup> For a well-argued appeal for a national credit report freeze law, see Kristan T. Cheng, *Identity Theft and the Case for a National Credit Report Freeze Law*, 12 N.C. BANKING INST. 239 (2008).

<sup>91</sup> Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

<sup>92</sup> Fair Credit Reporting Act of 1970, 15 U.S.C. §1681a(q)(3) (West 2000 & Supp. 2007).



agencies to develop guidelines and prescribe regulations for use by banks, credit unions, and other creditors for the purpose of identifying and preventing identity theft related risks to consumers.<sup>93</sup> In compliance with the requirements of the FACT Act, the FTC and the federal banking agencies developed and recently issued its Red Flags Rule, the subject of this section.<sup>94</sup>

This section of the note will first give a general overview of the Red Flags Rule. It will then discuss the major considerations a covered entity should adhere to when developing its Identity Theft Prevention Program and will thereafter discuss the four functions that the Program must adequately perform. Next, the section will describe the duties of card issuers regarding changes in address as well as duties of users of consumer reports regarding address discrepancies. Finally, this section will close with a discussion of how the rule alters the identity theft cat-and-mouse game.

#### A. GENERAL OVERVIEW

The Red Flags Rule was issued on October 3, 2007<sup>95</sup> and implements sections 114 and 315 of the FACT Act.<sup>96</sup> The final rules became effective on January 1, 2008. All covered financial institutions and creditors were originally required to be in compliance

---

<sup>93</sup> 15 U.S.C. §§ 1681m(e) & 1681c(h).

<sup>94</sup> Red flags are best understood as possible risks to account holders or customers or to the safety and soundness of the institution. They are patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. For a partial list of possible red flags, see *infra*, note 111.

<sup>95</sup> Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,717 (Nov. 9, 2007) (to be codified at 12 C.F.R. pt. 41, 12 C.F.R. pt. 222, 12 C.F.R. pts. 334 & 364, 12 C.F.R. pt. 571, 12 C.F.R. pt. 717 and 16 C.F.R. pt. 681), *available at* <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf> [hereinafter Red Flags Rule].

<sup>96</sup> Section 114 of the FACT Act amended section 615 of the FCRA and directed the Agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including special regulations requiring debit and credit card issues to validate notification of changes of address. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1960-61. Section 315 of the FACT Act added a new section to the FCRA that requires the Agencies to issue joint regulations that provide guidelines on reasonable policies and procedures that users of consumer reports should employ when they receive a notice of address discrepancy from a credit reporting agency. 117 Stat. 1996.

by November 1, 2008,<sup>97</sup> although the FTC has decided to suspend enforcement until May 1, 2009 to give creditors and financial institutions under its oversight “additional time in which to develop and implement written identity theft prevention programs.”<sup>98</sup> The delay in enforcement only extends to the development and implementation of an Identity Theft Prevention Program and does not alter the enforcement deadline of the rules regarding address discrepancies or changes of address.<sup>99</sup>

The rule requires any holder of a consumer account for which there is a reasonably foreseeable risk of identity theft (i.e. financial institutions, creditors) to develop and implement an Identity Theft Prevention Program (“Program”) for combating identity theft in connection with the opening of a new covered account or activity relating to existing covered accounts. It also provides guidelines on what such a program must include, but adopts a flexible, risk-based approach similar to that used in the Safeguards Rule<sup>100</sup> under the Gramm-Leach-Bliley Act.<sup>101</sup> The rule also requires credit and debit card issuers to develop policies and procedures to assess the validity of a consumer’s request for a change of address. Finally, the rule requires users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer reporting agency.

The Red Flags Rule addresses head-on the Task Force’s goal of making it more difficult for identity thieves who obtain consumer data to use it to steal identities. If effective, the Red Flags Rule should aid in lessening the incidence of both existing account fraud, the most prevalent form of identity theft, and new account fraud, the less prevalent, but more costly, form of identity theft. Financial

---

<sup>97</sup> Red Flags Rule, 72 Fed. Reg. at 63,718.

<sup>98</sup> Press Release, Fed. Trade Comm’n, FTC Will Grant Six-Month Delay of Enforcement of ‘Red Flags’ Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs (Oct. 22, 2008), *available at* <http://www.ftc.gov/opa/2008/10/redflags.shtm> [hereinafter FTC Press Release]. Note that the FTC’s decision to suspend enforcement does not affect other federal agencies’ enforcement of the original deadline for institutions subject to their oversight. FTC Enforcement Policy: Identity Theft Red Flags Rule, 16 C.F.R. § 681.2, <http://www.ftc.gov/os/2008/10/081022idtheftredflagsrule.pdf> (last visited Feb. 8, 2009).

<sup>99</sup> *Id.*

<sup>100</sup> 16 C.F.R. § 314.

<sup>101</sup> 15 U.S.C. §§ 6801–6809.

institutions all across the country have begun the process of developing the required programs.<sup>102</sup> Only time will tell how effective the Identity Theft Prevention Programs will be.

## B. RULES IMPLEMENTING SECTION 114

### 1. Identity Theft Prevention Program

The final rules describe who is required to develop a Program, the objectives of such a Program, the elements that the Program must contain, and how the Program must be administered. Under the rule, only financial institutions<sup>103</sup> and creditors<sup>104</sup> that offer or maintain “covered accounts”<sup>105</sup> must develop and maintain a written Program. Financial institutions and creditors must reassess their status every year to determine whether they come under the “covered account” application.<sup>106</sup> While the types of entities that are subject to the rule

---

<sup>102</sup> To help in these efforts, the FTC actively conducted outreach efforts to explain the rule to the many entities that come under its purview. As part of this effort, the FTC published a general alert of what types of entities are subject to the new rule. FED. TRADE COMM’N, NEW ‘RED FLAG’ REQUIREMENTS FOR FINANCIAL INSTITUTIONS AND CREDITORS WILL HELP FIGHT IDENTITY THEFT, FTC BUSINESS ALERT (2008), <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alto50.pdf> [hereinafter FTC BUSINESS ALERT].

<sup>103</sup> “Financial institution” is defined as a “state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a ‘transaction account’ belong to a consumer.” FTC BUSINESS ALERT, *supra* note 102.

<sup>104</sup> “Creditor” is “any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.” FTC BUSINESS ALERT, *supra* note 102.

<sup>105</sup> The rule defines a “covered account” as one that is either primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions or any other account for which there is a reasonably foreseeable risk of identity theft. Red Flags Rule, 72 Fed. Reg. at 63,719. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. FTC BUSINESS ALERT, *supra* note 102. Many institutions may already have similar policies and procedures in place as a result of their compliance with the customer identification program (“CIP”) regulations implementing Section 326 of the USA PATRIOT Act. See 31 C.F.R. § 103.121 (2007).

<sup>106</sup> Red Flags Rule, 72 Fed. Reg. at 63,719. As part of that assessment, every covered entity must conduct a risk assessment taking into consideration the methods it provides to open

may initially seem relatively straightforward, many entities that did not expect to be subject to the rule were rudely awakened to find that they too must develop Identity Theft Prevention Programs.<sup>107</sup> It was this confusion that led the FTC to forego enforcement for six months.<sup>108</sup>

The Program must be able to detect, prevent, and mitigate identity theft in connection with both new and existing covered accounts. However, not all Programs will be equally complex or thorough—the rule allows the Program to be tailored to the entity’s size and the complexity of its operations.<sup>109</sup>

Although the rule is flexible, it does require that four elements be included in all Programs. Every Program must contain “reasonable policies and procedures” to: (1) identify red flags for covered accounts and incorporate those red flags into the program; (2) detect the red flags once they have been incorporated into the Program; (3) respond to the red flags when detected so as to prevent and mitigate identity theft; and (4) ensure that the Program is updated each year in a way that reflects changes in the risk of identity theft. Further, financial institutions and creditors must follow mandatory steps in administering the program. Each entity must obtain approval of the initial written Program from its board of directors or a committee of the board.<sup>110</sup> Each entity must also ensure oversight of the development, implementation, and administration of the Program, ensure training of staff, and oversee service provider arrangements to assure compliance. The Agencies also issued guidelines to assist financial institutions and creditors in developing and implementing a program and a supplement that provides twenty-six examples of red

---

its accounts, the methods it provides to access its accounts, and its previous experience with identity theft. *Id.*

<sup>107</sup> For instance, non-profit and government entities that defer payment for goods or services are “creditors” that must comply with the rules. FTC BUSINESS ALERT, *supra* note 102.

<sup>108</sup> FTC Press Release, *supra* note 98.

<sup>109</sup> While an institution or creditor may determine that particular guidelines are not appropriate to incorporate into its program, every Program must contain reasonable policies and procedures to meet the specific requirements of the final rules. Red Flags Rule, 72 Fed. Reg. at 63,720.

<sup>110</sup> This is expected to ensure oversight of the development and implementation of the program.

flags that financial institutions and creditors should consider incorporating into their Programs.<sup>111</sup>

## 2. Validity of Change of Address Notifications

The Red Flags Rule also requires credit and debit card issuers to develop policies and procedures to assess the validity of a consumer's request for a change of address if it is shortly followed by a request for a replacement card. In accordance with section 114 of the FACT Act, the regulation provides that, if a card issuer receives notification of a change of address for a consumer's debit or credit card account, and within 30 days also receives a request for an additional or replacement card, the card issuer may not issue such card until the card issuer takes one of three steps: (1) notifies the cardholder of the request at the cardholder's former address, (2) notifies the cardholder by any other means of communication previously agreed to by the card issuer, or (3) otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to its Program.<sup>112</sup> Again, card issuers are provided with flexibility in formulating the policies and procedures required to maintain compliance with the regulation.

## C. RULE IMPLEMENTING SECTION 315

The rule implementing section 315 provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy. A "notice of address discrepancy" is defined as "a notice sent to a user of a consumer report by a CRA pursuant to 15 U.S.C. § 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer provided

---

<sup>111</sup> Some of these red flags include instances where: (1) a new revolving credit account is used in a manner commonly associated with known fraud patterns such as where the customer fails to make the first payment or makes an initial payment but no subsequent payments; (2) a covered account is used in a manner that is not consistent with established patterns of activity on the account; (3) personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer (e.g., there is a lack of correlation between the SSN range and date of birth); and (4) the majority of available credit is used for cash advances or merchandise that is easily convertible to cash. *See, e.g.*, Red Flags Rule, 72 Fed. Reg. at 63,770–71.

<sup>112</sup> Red Flags Rule, 72 Fed. Reg. at 63,772.

by the user in requesting the consumer report and the address or addresses the CRA has in the consumer's file."<sup>113</sup>

The Rule provides that a user of a consumer report must "develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy."<sup>114</sup> One such procedure might include that of comparing the information in the consumer report with other information the user has on the consumer. This information may come from one of several sources: (1) that which the user obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program rules implementing 31 U.S.C. § 5318(l), (2) that which the user maintains in its own records, or (3) that which the user obtains from third party sources. Alternatively, the user could verify the information directly with the consumer.

#### D. POUNCE OR ESCAPE?

The word that best describes the Red Flags Rule is "flexible." In fact, consumer groups that responded to the Agencies' request for comment<sup>115</sup> voiced concerns that the proposed rule was too flexible. Indeed, the final rule is even more flexible than that which was submitted for comment. As the consumer groups contended, this flexibility may encourage business as usual. Of course, no one-size-fits-all rule would be appropriate. The FACT Act, and the regulations promulgated pursuant to the statute, is intended to address the needs of consumers while providing for the efficient operation of the national credit market.<sup>116</sup> The flexible framework gives organizations

---

<sup>113</sup> Red Flags Rule, 72 Fed. Reg. at 63,771.

<sup>114</sup> *Id.*

<sup>115</sup> The Agencies published a joint notice of proposed rulemaking in the Federal Register at 71 Fed. Reg. 40,786 on July 18, 2006, proposing rules and guidelines to implement section 114 and proposing rules to implement section 315 of the FACT Act. The public comment period closed on September 18, 2006. The Agencies received a total of 129 comments. The comments came from sixty-three financial institutions, twelve financial institution holding companies, twenty-three financial institution trade associations, twelve individuals, nine other trade associations, five other business entities, three consumer groups, one member of Congress, and one from the United States Small Business Administration. Red Flags Rule, 71 Fed. Reg. at 63,718.

<sup>116</sup> S. Rep. No. 108-166, at 2 (2003).

the discretion to implement techniques and procedures that are the most appropriate for their respective business environments. It has been argued that such flexibility is necessary because the businesses are best positioned to understand the types of security measures that are the most appropriate for their particular situations and the particular information they maintain.<sup>117</sup>

The flexible approach of the Red Flags Rule resembles that promoted by the Task Force for national data security and breach notification laws, and can be justified on the same grounds: as the costs associated with implementing the rule may be different depending on an entity's size, it is both necessary and beneficial for the rule to call for actions that are reasonable for that particular covered entity.<sup>118</sup> Still, if the flexible nature of the rule does indeed encourage business as usual, the Agencies (despite their best efforts) will have done very little to prevent identity theft. The mice will once again win the game. In some instances, strict rules are necessary in order to ensure the intended results.

Another problem recognized by the Agencies is that many of the red flags that are relevant today may become obsolete as time passes.<sup>119</sup> However, this potential problem is likely to be addressed, because the Agencies are expected to periodically update the guidelines.<sup>120</sup> Furthermore, the Rule provides that each covered institution must incorporate into its Program relevant red flags from applicable supervisory guidance, incidents of identity theft that the financial institution or creditor has experienced, and methods of identity theft that the institution has identified that reflect changes in identity theft risks. Therefore, a company's program should adequately reflect the most up-to-date indicators of identity theft.

Ultimately, the Red Flags Rule should help financial institutions and creditors better protect consumers by monitoring the accounts with an educated and watchful eye. One hopes that these institutions will take their responsibilities seriously and continue to update their

---

<sup>117</sup> A.B.A. SECTION OF ANTITRUST LAW, DATA SECURITY HANDBOOK, 105-20 (2008). *See also* S. Rep. No. 108-166, at 13 (2003) (noting the intent of the Committee that the guidelines provide flexibility "given the changing nature of identity theft and related crimes").

<sup>118</sup> STRATEGIC PLAN, *supra* note 6, at 37.

<sup>119</sup> Red Flags Rule, 72 Fed. Reg. at 63,726.

<sup>120</sup> Section 114 of the FACT Act directs the Agencies to update the guidelines as often as necessary. *See* 15 U.S.C. § 1681m(e)(1)(A).

Programs to reflect the growing sophistication of identity thieves. In doing so, the institutions will further the Task Force's goal of making it more difficult for identity thieves who obtain consumer data to use it to steal identities.

## V. CONCLUSION

The last year has proven to be a busy one for state legislatures and the regulating authorities, who have collectively continued in their efforts to keep up with the identity theft crisis. The Task Force concluded its Strategic Plan by noting that only a comprehensive and fully coordinated strategy that encompasses effective prevention, public awareness and education, victim assistance, and law enforcement measures at all levels of government will have any chance at solving the problem of identity theft. Although the progress of the last year is only a part of that plan, and certainly not all that is needed, it has provided consumers with significant protection. Still, the cat-and-mouse-game will continue. To quote the Task Force, "[t]here is no magic bullet that will eradicate identity theft."<sup>121</sup> The government must continue to find and implement more effective means of protecting the identities of its citizens.

---

<sup>121</sup> STRATEGIC PLAN, *supra* note 6, at 72.



## APPENDIX A

The table on the following six pages highlights some of the important distinguishing characteristics of the state security freeze statutes. Below are a few notes to help read the Table:

1. Availability column: Addresses whether a security freeze can be requested by all consumers or only identity theft victims (“IDTV”).
2. Freeze Length column: Addresses whether a freeze on a consumer’s credit report is unlimited or automatically expires after the passing of years.
3. Electronic Request column: Addresses whether the state statutes require that CRAs accept freeze requests electronically or by methods other than certified mail.
4. Initial Response column: Addresses the length of time a CRA has to respond to a request for the initial security freeze on a consumer’s report. All time periods refer to business days.
5. Temporary Lift/Response column: Addresses whether a consumer can request that a freeze be temporarily lifted for a specific amount of time only (“time”), for a specific party only (“specific party”), or for either a specific amount of time or for a specific party, at the consumer’s option (“both”). This column also addresses the amount of time that a CRA is allowed to respond to a consumer request to temporarily lift a freeze.
6. Allowed Charges column: Addresses the charges that a CRA is statutorily allowed to charge a consumer requesting a freeze.

<u>State</u>	<u>Statute Citation</u>	<u>Availability</u>	<u>Freeze Length</u>	<u>Electronic Request</u>	<u>Initial Response</u>	<u>Temporary Lift/Response</u>	<u>Allowed Charge</u>
Ala.	NO LAW	NA	NA	NA	NA	NA	NA
Alas.	H.B. 65, 25 <sup>th</sup> Leg., 2d Reg. Sess. (Ala. 2008) (to be Codified at ALASKA STAT. § 45.48.100, et. seq.)	Consumers	Unlimited	Only if CRA has made available; otherwise certified mail only	5 days	Specific party; 3 days; 15 minutes if requested electronically or by phone	\$5 to place; \$2 to temp. lift; none for IDTV
Ariz.	S.B. 1185, 48 <sup>th</sup> Leg. 2d Reg. Sess. (Ariz. 2008) (to be codified at Ariz. REV. STAT. ANN. § 44-1695)	Consumers	Unlimited	Certified or regular mail only	10 days	Time; 3 days; 15 minutes if requested electronically or by phone	\$5 each request; none for IDTV
Ark.	ARK. CODE ANN. § 4-112-101, et. seq. (2001 & Supp. 2007)	IDTV only (see definition of "consumer")	Unlimited	Certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and respond to requests	\$10 each request
Cal.	CAL. CIV. CODE § 1785.11.2, et. seq. (West 1998 & Supp. 2008)	Consumers	Unlimited	Certified or regular mail only	5 days	Both; 3 days	\$10 each request; \$5 each request if 65+; none for IDTV
Colo.	COLO. REV. STAT. § 12-14.3-106.6, et. seq. (2008)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	None for initial placement; \$10 to lift for period of time, remove, or subsequent placement; \$12 to lift for specific party
Conn.	CONN. GEN. STAT. § 36a-701-701a (2004 & Supp. 2008)	Consumers	Unlimited	Only if CRA has made available; otherwise certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$10 to place, lift for period of time, or remove; \$12 to lift for specific party
Del.	DEL. CODE ANN. tit. 6 § 2203 (2005 & Supp. 2006)	Consumers	Unlimited	Available as of Jan. 31, 2009	3 days	Time; 3 days; 15 minutes if requested electronically or by phone	\$20 for initial placement; none otherwise; none for IDTV
D.C.	D.C. CODE § 28-3861-	Consumers	Unlimited	Available as of Jan. 31,	3 days	Both; 3 days; 15 minutes if	\$10 for initial placement;

<u>State</u>	<u>Statute Citation</u>	<u>Availability</u>	<u>Freeze Length</u>	<u>Electronic Request</u>	<u>Initial Response</u>	<u>Temporary Lift/Response</u>	<u>Allowed Charge</u>
	3862 (LexisNexis 2001 & Supp. 2008)			2009		requested electronically or by phone	none otherwise; none for IDTV
Fla.	FLA. STAT. ANN. § 501.005 (West 2006 & Supp. 2008)	Consumers	Unlimited	Certified mail only	5 days	Time; 3 days; 15 minutes if requested electronically or by phone	\$10 each request; none for IDTV; none for 65+ for initial placement or for removal
Ga.	GA. CODE ANN. § 10-1-913, et. seq. (2008)	Consumers	Unlimited	Available as of Aug. 1, 2008	3 days	Time; 3 days; 15 minutes if requested electronically or by phone	\$3 each request; none for IDTV or 65+
Haw.	HAW. REV. STAT. § 489P-1, et. seq. (2008)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days	\$5 each request; none for IDTV
Idaho	IDAHO CODE ANN. § 28-52-101, et. seq. (1999 & Supp. 2008)	Consumers	Unlimited	Certified mail only	3 days	Both; 3 days; 15 minutes if requested electronically or by phone	\$6 to place or temp. lift; none to remove; none for IDTV
Ill.	815 ILL. COMP. STAT. 505/2MM (West 1999 & Supp. 2008)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days	\$10 each request; none for IDTV or 65+
Ind.	IND. CODE § 24-5-24-1, et. seq. (West 2006 & Supp. 2008)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days; as of Jan. 1, 2009, 15 minutes if requested electronically or by phone	No fees
Iowa	S.F. 2277, 82d Gen. Assem. (Iowa 2008) (to be codified at IOWA CODE § 714F.1, et. seq.)	Consumers	Unlimited	Certified mail only	5 days	Time; 3 days; 15 minutes if requested electronically or by phone	\$10 to place or remove; \$12 to temp. lift; none for IDTV
Kan.	KAN. STAT. ANN. § 50-723, et. seq. (2008)	IDTV only	Unlimited	Certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and respond to requests	Not stipulated
Ky.	KY. REV. STAT. ANN. § 367.363, et. seq. (2008)	Consumers	7 years	Certified mail only	10 days	Time; 3 days; encourages expedited methods to receive and respond to requests	\$10 each request

<u>State</u>	<u>Statute Citation</u>	<u>Availability</u>	<u>Freeze Length</u>	<u>Electronic Request</u>	<u>Initial Response</u>	<u>Temporary Lift/Response</u>	<u>Allowed Charge</u>
La.	LA. REV. STAT. ANN. art. 9 § 3571.1 (1997 & Supp. 2008)	Consumers	Unlimited	Certified mail only	10 days	Time; 3 days	\$10 to place; \$8 to temp. lift; no fee to remove; none for IDTV or 62+
Me.	ME. REV. STAT. ANN. tit. 10 § 1313-C, et. seq. (1997 & Supp. 2007)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$10 to place, lift for period of time, or remove; \$12 to lift for specific party; none for IDTV
Md.	MD. CODE ANN., COM. LAW § 14-1212.1 (2005 & Supp. 2008)	Consumers	Unlimited	Only if CRA has made available; otherwise certified mail only; phone option starting Jan. 1, 2010	3 days	Both; 3 days; as of Jan. 31, 2009, 15 minutes if requested electronically or by phone	\$5 each request; none for IDTV
Mass.	MASS. GEN. LAWS ch. 93 § 62A, et. seq. (2005 & Supp. 2008)	Consumers	Unlimited	Certified, overnight, or regular mail only	3 days	Both; 3 days	\$5 each request; none for IDTV or spouse of IDTV
Mich.	NO LAW	NA	NA	NA	NA	NA	NA
Minn.	MINN. STAT. § 13C.016, et. seq. (2005 & Supp. 2008)	Consumers	Unlimited	Only if CRA has made available; otherwise certified mail or by telephone	3 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$5 each request; none for IDTV
Miss.	MISS. CODE ANN. § 75-24-201, et. seq. (West 1999 & Supp. 2007)	IDTV only	Unlimited	Certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$10 to place; none otherwise
Mo.	NO LAW	NA	NA	NA	NA	NA	NA
Mont.	MONT. CODE ANN. § 30-14-1726, et. seq. (2007)	Consumers	Unlimited	Available as of Jan. 31, 2009	5 days; 24 hours if requested by IDTV	Both; 3 days; as of Jan. 31, 2009, 15 minutes if requested electronically or by phone	\$3 to place or lift; none to remove; none for IDTV
Neb.	NEB. REV. STAT. § 8-2601, et. seq. (2003 & Supp. 2008)	Consumers	7 years	Certified mail only	3 days	Time; 3 days; as of Jan. 1, 2009, 15 minutes if requested electronically or by phone	\$15 to place; none otherwise; none for minor or IDTV
Nev.	NEV. REV. STAT. ANN. §	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days; encourages	\$10 each request; none

<u>State</u>	<u>Statute Citation</u>	<u>Availability</u>	<u>Freeze Length</u>	<u>Electronic Request</u>	<u>Initial Response</u>	<u>Temporary Lift/Response</u>	<u>Allowed Charge</u>
	598C.300, et. seq. (LexisNexis 2004 & Supp. 2007)					expedited methods to receive and respond to requests	for IDTV or 65+
N.H.	N.H. REV. STAT. ANN. § 359-B:22, et. seq. (1995 & Supp. 2008)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$10 each request; none for IDTV
N.J.	N.J. STAT. ANN. § 56:11-44, et. seq. (2001 & Supp. 2008)	Consumers	Unlimited	Only if CRA has made available; otherwise certified mail only	5 days	Both; 3 days; mandates development of expedited methods; goal response time set at 15 minutes	None to place; \$5 to lift or remove
N.M.	N.M. STAT. § 56-3A-3 (LEXISNEXIS 2004 & SUPP. 2008)	Consumers	Unlimited	Only if CRA has made available; otherwise certified or regular mail only	3 days	Both; 3 days; as of Sept. 1, 2008, 15 minutes if requested electronically or by phone	\$10 to place; \$5 to lift or remove; none for 65+ or IDTV
N.Y.	N.Y. GEN. BUS. LAW § 380-t (McKinney 1996 & Supp. 2008)	Consumers	Unlimited	Certified or overnight mail only	3 days; beginning Jan. 1, 2010, 24 hours	Both; 3 days; encourages expedited methods to receive and respond to requests	None for initial placement; \$5 each request thereafter; none for IDTV
N.C.	N.C. GEN. STAT. ANN. § 75-63 (2007)	Consumers	Unlimited	Certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and respond to requests	\$10 each request; none for IDTV
N.D.	N.D. CENT. CODE § 51-33-01, et. seq. (2007)	Consumers	Unlimited	Only if CRA has made available; otherwise certified mail or telephone only	3 days; beginning Aug. 1, 2009, 48 hours if requested by IDTV	Both; 3 days; encourages expedited methods to receive and respond to requests, with goal of 15 minutes if requested electronically or by phone	\$5 to place or lift; none to remove; none for IDTV
Ohio	H.B. 46, 127th Gen. Assem. (Ohio 2008) (to be codified at	Consumers	Unlimited	Certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and	\$10 each request; none for IDTV

<u>State</u>	<u>Statute Citation</u>	<u>Availability</u>	<u>Freeze Length</u>	<u>Electronic Request</u>	<u>Initial Response</u>	<u>Temporary Lift/Response</u>	<u>Allowed Charge</u>
	OHIO REV. CODE ANN. § 1349.52)					respond to requests	
Okla.	OKLA. STAT. tit. 24 § 149, et. seq. (2008)	Consumers	Unlimited	Certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and respond to requests	\$10 each request; none for IDTV; none to place or remove for 65+
Or.	OR. REV. STAT. § 646A.606, et. seq. (2007)	Consumers	Unlimited	Only if CRA has made available; otherwise certified or regular mail only	5 days	Time; 3 days; time limits to have been reviewed and reassessed by end of 2008	\$10 each; none IDTV
Pa.	73 PA. CONS. STAT. § 2501, et. seq. (2008)	Consumer	7 years	Only if CRA has made available; otherwise certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$10 to place or lift; none to remove; none for IDTV; none to place for 65+
R.I.	R.I. GEN. LAWS § 6-48-1, et. seq. (2001 & Supp. 2007)	Consumer	Unlimited	Certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and respond to requests	\$10 each request; none for IDTV or 65+
S.C.	S.C. CODE ANN. § 37-20-160 (2008)	Consumer	Unlimited	Available as of Dec. 31, 2008	5 days	Both; 15 minutes if requested electronically or by phone	No fee
S.D.	S.D. CODIFIED LAWS § 54-15-1, et. seq. (2004 & Supp. 2008)	IDTV only	7 years	Certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and respond to requests	No fees
Tenn.	TENN. CODE ANN. § 47-18-2108 (2001 & Supp. 2007)	Consumers	Unlimited	Available as of Jan. 31, 2009	3 days	Time; 15 minutes if requested electronically or by phone	\$7.50 to place; none to lift; \$5 to remove; none for IDTV
Tex.	TEX. BUS. & COM. CODE ANN. § 20.01, et. seq. (Vernon 2002 & Supp. 2008)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$10 to place, lift for period of time, or remove; \$12 to lift for specific party; none for IDTV
Utah	UTAH CODE ANN. § 13-45-201, et. seq.	Consumers	Unlimited	Certified mail only	5 days	Time; 3 days; 15 minutes if requested	"Reasonable" fee to place or lift; none

<u>State</u>	<u>Statute Citation</u>	<u>Availability</u>	<u>Freeze Length</u>	<u>Electronic Request</u>	<u>Initial Response</u>	<u>Temporary Lift/Response</u>	<u>Allowed Charge</u>
	(2008)					electronically or by phone	for IDTV
Vt.	VT. STAT. ANN. tit. 9, § 2480h, et. seq. (2006)	Consumers	Unlimited	Certified mail only	5 days	Both; 3 days; encourages expedited methods to receive and respond to requests	\$10 to place, \$5 to lift or remove; none for IDTV
Va.	VA. CODE ANN. 59.1.-444.1, et. seq. (2006 & Supp. 2008)	Consumers	Unlimited	Certified mail only	3 days	Both; 3 days; as of Sept. 1, 2008, 15 minutes if requested electronically or by phone	\$10 to place; none otherwise; none for IDTV
Wash.	WASH. REV. CODE § 19.182.170 (2007 & Supp. 2008)	As of Sept. 1, 2008, all consumers	Unlimited	Certified mail only	5 days	Time; 3 days; as of Sept. 1, 2008, 15 minutes if requested electronically or by phone	\$10 each request; none for IDTV or 65+
W. Va.	W. VA. CODE § 46A-6L-101, et. seq. (LexisNexis 2006 & Supp. 2008)	Consumers	Unlimited	Available as of Jan. 31, 2009	5 days	Time; 3 days; as of Sept. 1, 2008, 15 minutes if requested electronically or by phone	\$5 each request; none for IDTV
Wis.	WIS. STAT. § 100.54 (2004 & Supp. 2007)	Consumers	Unlimited	Only if CRA has made available; otherwise certified mail only	5 days	Time; 3 days; encourages expedited methods to receive and respond to requests	\$10 each request; none for IDTV
Wyo.	WYO. STAT. ANN. § 40-12-501, et. seq. (2007)	Consumers	Unlimited	Certified mail only	5 days	Time; 3 days; as of Sept. 1, 2008, 15 minutes if requested electronically or by phone	\$10 each request; none IDTV

